EXHIBIT 49

```
1        UNITED STATES DISTRICT COURT
2        SOUTHERN DISTRICT OF NEW YORK
3
4   SECURITIES AND EXCHANGE    )
    COMMISSION,            )
5                          )
         Plaintiff,    )
6                      ) Case No.
     vs.               ) 23-cv-9518-PAE
7                      )
    SOLARWINDS CORP. and     )
8   TIMOTHY G. BROWN,        )
                         )
9        Defendants.   )
    _____)
10
11
12
13        VIDEOTAPED DEPOSITION OF
14            BRAD CLINE
15           Austin, Texas
16       Tuesday, October 1, 2024
17
18
19
20
21
22
23
24  Reported by:
    Micheal A. Johnson, RDR, CRR
25  Job No. 241001MJ
```

1

```
1        UNITED STATES DISTRICT COURT
2        SOUTHERN DISTRICT OF NEW YORK
3
4   SECURITIES AND EXCHANGE   )
    COMMISSION,            )
5                          )
         Plaintiff,    )
6                      ) Case No.
     vs.               ) 23-cv-9518-PAE
7                      )
    SOLARWINDS CORP. and     )
8   TIMOTHY G. BROWN,        )
                         )
9        Defendants.   )
    _____)
10
11
12
13
14        Videotaped deposition of BRAD CLINE, taken
15  on behalf of Plaintiff, at Latham & Watkins, LLP,
16  300 Colorado Street, Suite 2400, Austin, Texas,
17  beginning at 9:07 a.m. and ending at 5:05 p.m. on
18  October 1, 2024, before Micheal A. Johnson, a
19  Registered Diplomate Reporter, Certified Realtime
20  Reporter, and Notary Public of the State of Texas.
21
22
23
24
25
```

2

```
1   APPEARANCES:
2   ON BEHALF OF PLAINTIFF:
3       U.S. SECURITIES AND EXCHANGE COMMISSION
        BY: Kristen M. Warden
4           John J. Todor
            Christopher J. Carney
5       100 F Street, NE
        Washington, D.C. 20549
6       (202) 256-7941
        wardenk@sec.gov
7       todorj@sec.gov
        carneyc@sec.gov
8
9   ON BEHALF OF DEFENDANTS
    SOLAR WINDS CORP. AND TIMOTHY G. BROWN:
10
        LATHAM & WATKINS LLP
11      BY: Serrin Turner
            Joshua A. Katz
12      1271 Avenue of the Americas
        New York, New York 10020
13      (212) 906-1330
        serrin.turner@lw.com
14      josh.katz@lw.com
15
    ALSO PRESENT:
16
        Becky Melton
17      Jason Bliss
        Annie Gravelle (Via Zoom)
18
19  VIDEOGRAPHER:
20      Timothy Desadier
21
22
23
24
25
```

3

```
1               INDEX
               BRAD CLINE
2             October 1, 2024
3
    APPEARANCES                    3
4
    PROCEEDINGS                    7
5
6
    EXAMINATION OF BRAD CLINE:
7
    BY MS. WARDEN                  8
8
9
    REPORTER'S CERTIFICATION       233
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
```

4

1 end user services team. See if there's any else in
2 the initial -- in my return. I believe those are
3 the main teams that I had under me in -- as of
4 October, when I rejoined the company.
5   **Q.**   October of 2020?
6   **A.**   Yes, correct.
7   **Q.**   Okay. And let's just break that up. So
8 the -- what did the networking team that you managed
9 do?
10   **A.**   Networking team managed all -- manages
11 and managed all of our internal networking to the
12 corporate side of IT, including connectivity to the
13 Internet, and if there was any SaaS or cloud-based
14 networking within AWS or Azure, they would also
15 manage that networking.
16   **Q.**   Okay. And what did the systems team do?
17   **A.**   The systems team managed what we would
18 call our primary server systems for corporate IT.
19 So in the scope for corporate IT that would be
20 on-premise, any of our servers that were on-prem,
21 Active Directory. They would also manage oversight
22 of our AWS and any other cloud such as Google or
23 Azure for corporate IT.
24   **Q.**   Okay. And then you also managed the UC
25 team. What was that?

13

1   **A.**   UC is unified communications. So it's
2 audio/visual and then also anything phone systems.
3   **Q.**   And you also managed the end user
4 services team.
5   What did that team do?
6   **A.**   End user services is basically your
7 standard user for -- so employee, internal employee
8 or -- we would call our customers, but our internal
9 employees, and it would be handling any of their
10 support needs. So new laptop, provisioning,
11 onboarding, offboarding, you know, mouse breaks,
12 those kinds of things.
13   **Q.**   And about how many people do you
14 currently manage as senior director of IT?
15   **A.**   In the current role, which I now handle
16 the business application group, which is a different
17 team, it's roughly 97 folks last time I checked. In
18 my prior role over IT operations it was a little
19 over 100, about 105, 110 with contractors.
20   **Q.**   So do you no longer manage the networking
21 systems, UC and end service -- end user services
22 teams?
23   **A.**   I do not as of March of this year.
24   **Q.**   Okay. So let's talk about head of -- in
25 March 2024 you transitioned to be the head of

14

1 BizApps?
2   **A.**   Yes, that's correct.
3   **Q.**   So who's the current senior director of
4 IT?
5   **A.**   Brody Taylor.
6   **Q.**   And what were you hired to do as the head
7 of BizApps?
8   **A.**   The role for business applications is
9 very focused on what it sounds like, they're our
10 business applications. So it's primarily if you
11 think of Salesforce, NetSuite, our HR and marketing
12 application. So it's very much focused on the
13 application side that the business runs off of.
14   **Q.**   And just focusing on your time as senior
15 director of IT, October 2020 to March 2024, what was
16 your role at the company in connection with
17 cybersecurity?
18   **A.**   In general, my team would handle the
19 implementation of policies. So if you had a policy
20 around onboarding or offboarding, that may have been
21 approved and handled by the compliance team and
22 InfoSec team, then we would do the general
23 enforcement or the daily processes around that
24 procedure, was generally how we handled that.
25   But there's many -- there are many facets

15

1 to that. Networking team had firewalls. Firewalls
2 obviously have a large security component to them.
3 All your servers and applications, patching, all of
4 those have security implications.
5   **Q.**   And you mentioned implementation of
6 policies. Did you draft any of the policies?
7   **A.**   I've been part of drafting some basic
8 policies, can't remember specifically, but generally
9 those -- all those policies are created either at
10 the InfoSec or compliance team or legal teams. So
11 not a general part of my role. I would consult or
12 provide information as of feasibility or
13 implementation options was generally how my role
14 would play.
15   **Q.**   Okay. And then as senior director of IT,
16 who did you report to?
17   **A.**   Initially I reported to Rani Johnson and
18 then --
19   **Q.**   And what was her position?
20   **A.**   She was CIO. And then as she
21 transferred -- or left the company, I reported to
22 Chris Day, also a CIO.
23   **Q.**   Okay. And as head of BizApps, you report
24 to Mr. Day?
25   **A.**   Yes, that's correct.

16

1   Q.   And then let's -- if you go down to --
2 looks like you left SolarWinds in November 2019,
3 right?
4   A.   Yes, that's correct.
5   Q.   Okay. And you joined EZCORP?
6   A.   EZCORP, correct, yes.
7   Q.   And what was EZCORP?
8   A.   It is a financial banking company in that
9 sector.
10   Q.   And what was your role as VP of
11 infrastructure?
12   A.   At that business I had both what would be
13 considered the business applications and the
14 infrastructure teams, managing all of their
15 infrastructure and external customer-facing systems.
16   Q.   Okay. And then focusing in on the bottom
17 of your LinkedIn profile, prior to leaving for
18 EZCORP it says that you worked at SolarWinds between
19 May -- October 2016 and November 2019; is that
20 right?
21   A.   Yes, that sounds correct.
22   Q.   Okay. So let's split it up. Two
23 different positions, right?
24   A.   Yes, I had two different positions.
25 Different teams during that time as well.

17

1   Q.   Okay. So you joined SolarWinds in
2 October 2016 as a senior manager, right?
3   A.   Correct.
4   Q.   And was it a senior manager in the IT
5 group?
6   A.   That is correct, yeah. States there I
7 was the manager of the network engineering team.
8   Q.   Okay. And what did you do as the manager
9 of the network engineering team?
10   A.   The network team as mentioned handled all
11 of our internal corporate network systems. That
12 would be your switching and routing, firewalls for
13 the company.
14   Q.   Okay. And who did you report to as
15 senior manager IT?
16   A.   Originally it was Jason Matthews.
17   Q.   Okay. And then in May 2017 you
18 transitioned to be director of information
19 technology at SolarWinds; is that correct?
20   A.   Correct.
21   Q.   Okay. And you held that position until
22 November 2019?
23   A.   Correct.
24   Q.   Okay. How did your duties change as
25 director of information technology at SolarWinds?

18

1   A.   I had handled -- or I took on the systems
2 team at that time initially, and I reported to Dave
3 Mills, was my initial reporting.
4   Q.   And what was Mr. Mills' position?
5   A.   He was VP of information technology at
6 that time.
7   Q.   Okay. At some point did you report to
8 the CIO Rani Johnson?
9   A.   I did, and there was a period there that
10 I also -- I had reported to Bill Carroll, who was
11 senior director of IT.
12   Q.   And as director of information technology
13 at the company, what was your role in connection
14 with cybersecurity?
15   A.   Similar to previously stated. So I would
16 have had management of the end-user devices,
17 management of -- for corporate IT, the management of
18 our networking switches, firewalls, servers. And so
19 all of those, of course, have a security component
20 and we would follow the InfoSec and security and
21 compliance guidelines for implementation.
22   Q.   Did you interact with any SolarWinds
23 executives focusing in on your time as director of
24 IT, May 2017 to November 2019?
25   A.   Executives. Yes. I mean, there was

19

1 always either support capacity or there may have
2 been a project that we were working on or a
3 presentation. So there's always chances for
4 interactions.
5   Q.   And which ones?
6   A.   It would probably pretty much be anybody
7 at any point in time. We were a support
8 organization. So if somebody from sales needed
9 assistance, you know, an executive in sales, we
10 would go and support them. Marketing. If one of
11 the other leaders had a question around technical,
12 we also supported the company, we had some
13 initiatives around -- we as IT were very much
14 exemplary of our customers, because SolarWinds sells
15 software to customers very much similar sized IT as
16 our organization. And so we provide feedback on
17 products that we thought were of interest. We
18 provide feedback on needs that we had as a team that
19 we could see customers also needing.
20   So those were all different interactions
21 that we would have with executive teams. So maybe a
22 presentation on a feature or function within the
23 product that would be beneficial to us. So we would
24 show that and at times it would either be -- we
25 would be called into a group to give that

20

1   **Q.**   And how would you be aware that this was
2 happening?
3   **A.**   It would not be normally something in my
4 line of sight as a director.
5   **Q.**   But -- so how were you apprised of it?
6   **A.**   How was I apprised of it? That they were
7 testing? That was -- that was our normal processes.
8 If I go back to the point that I was a network
9 manager, I would have helped implement those
10 processes and then as a director it would not have
11 been a normal part of my job and duties. It would
12 have been my manager's job and duties. So if there
13 was a failure, that failure didn't deploy correctly,
14 oftentimes the manager of that team would let me
15 know, Hey, we're doing a big firewall upgrade, the
16 firewall upgrade did not go as planned, we had to
17 revert back, roll back to the prior version. We're
18 going to attempt it with a different change, a
19 different configuration. We're go to ask for
20 another change window on such-and-such date, I give
21 approval for that next change window and then go
22 forward.
23   That would be about as much as I would be
24 involved in that.
25   **Q.**   Mr. Cline, did you request that senior

65

1 management move to automated access rights
2 management product?
3   MR. TURNER: Objection to form.
4   **A.**   I'm sorry, I didn't catch -- catch it
5 fully.
6 BY MS. WARDEN:
7   **Q.**   Sure. Did you request that senior
8 management move to automated access rights
9 management product?
10   MR. TURNER: Objection to form.
11   **A.**   I can't remember specifically if we had
12 reviewed that product preacquisition, so I can't --
13 I can't say specifically. We may have identified an
14 area that we were looking to automate and they may
15 have gone and found that product, but I -- that
16 would be too far out of my scope.
17 BY MS. WARDEN:
18   **Q.**   Sorry, when we're referring to the
19 product, you mean the 8MAN, what is it, ARM?
20   **A.**   It was the 8MAN ARM product, Access
21 Rights Manager.
22   **Q.**   So you're not aware of the process and
23 how it was implemented at SolarWinds?
24   MR. TURNER: Objection to form.
25   **A.**   I was part of the implementation of the

66

1 product, yes.
2 BY MS. WARDEN:
3   **Q.**   Okay. And what does that mean?
4   **A.**   From the technical perspective, one of my
5 teams would have been responsible for installing it,
6 tying it into our systems and working on the
7 workflows that would have assisted with the
8 automation of some of the onboarding tasks.
9   **Q.**   But did you have any role in recommending
10 the 8MAN ARM product to senior management at
11 SolarWinds?
12   **A.**   I can't recall directly. I know there
13 were times that I was asked to review a product that
14 we may have been looking at from an acquisition
15 standpoint, if it was relevant to our team, if we
16 thought it was a piece of software that had
17 potential and how we would use it and we would give
18 examples, but I can't remember -- recall
19 specifically if we pretested ARM. I believe that
20 time frame was around 2018, so roughly six years
21 ago. I can't remember.
22   We did do presentations on them, so there
23 may be an artifact showing our feedback on that
24 product. And there were different members of my
25 teams, so I wasn't always necessarily included in

67

1 all the products that we reviewed for the company.
2   **Q.**   Okay. Before -- as your role as director
3 of IT, would you have typically been part of
4 reviewing a product with respect to access rights
5 management?
6   MR. TURNER: Object to form.
7   **A.**   I would say that's very contextual as
8 well. As mentioned, I can't remember precisely if I
9 reviewed ARM before we acquired it and I wasn't
10 always involved in every potential acquisition.
11 Some might have some intersection with my areas of
12 expertise and at times I would be consulted. Other
13 times I was not. Just wasn't part of my role
14 specifically.
15 BY MS. WARDEN:
16   **Q.**   Do you recall having any conversations
17 with Rani Johnson regarding implementing ARM at
18 SolarWinds?
19   **A.**   I believe we would have talked about it.
20 I can't remember specifically. We had -- I was
21 generally almost daily in her office at some point
22 or another for one meeting or another, so I can't
23 recall specifically if we talked about ARM. I know
24 we did talk about me traveling there for the
25 acquisition. So I actually visited Berlin when we

68

1 did the acquisition just to help greet the team, get
2 them set up for a WebEx so that KBT could talk to
3 them, but I can't remember what details we would
4 have talked about the product itself or the
5 implementation of the product.
6   Q.   Do you recall any conversations with Rani
7 Johnson regarding concerns about the manual process
8 for access rights management?
9   A.   No, I don't remember any specific context
10 around concerns. We were always looking for ways to
11 automate anything that was a manual task within IT
12 that allows you to do -- be more efficient and
13 effective. So we may have had a conversation around
14 automation of change management -- or facets of
15 change management because you can't automate all of
16 it.
17   In particular, SARF was one of the things
18 that we had looked at as an area that we could do
19 more automation in. But I can't recall specific
20 conversations with her.
21   Q.   Did you tell senior management that
22 manual process for access rights management was
23 inefficient?
24   A.   I don't recall having a conversation of
25 that nature.

69

1   Q.   Would you consider it to be a best
2 practice in the IT industry to have automated
3 process for access rights management?
4   MR. TURNER: Object to form.
5   A.   Sorry, can you restate?
6 BY MS. WARDEN:
7   Q.   Sure. Would you consider it to be a best
8 practice in the IT industry to have automated
9 processes for access rights management?
10   MR. TURNER: Object to form.
11   A.   In my opinion, it's -- and it's very
12 dependent on the software. A lot of tools have
13 changed over the time period that we're speaking of.
14 So it would be very dependent on the business, but
15 it is an area that when you automate, it can make
16 things more efficient. So I would say it's more of
17 an efficiency concern is where I would look at
18 automation. Automation can also have risks, so it's
19 a double-edged sword.
20 BY MS. WARDEN:
21   Q.   Okay. Would you consider automated
22 processes for access rights management to be a more
23 efficient vehicle?
24   MR. TURNER: Object to form.
25   A.   I would say it's more efficient from a

70

1 employee perspective, yes. As far as anytime you
2 automate something, it should take less people to do
3 that, so that's more efficient, yes.
4 BY MS. WARDEN:
5   Q.   Okay. Sir, can you take a look --
6 directing your attention to the Auditing and Logging
7 paragraph of Exhibit 3 [sic].
8   Do you see that?
9   A.   Yes.
10   Q.   Can you read that paragraph to yourself.
11   (Witness reviews document.)
12   A.   Yes. I read it.
13 BY MS. WARDEN:
14   Q.   Okay. So, Mr. Cline, is that paragraph
15 about auditing and logging true?
16   A.   As far as the areas that I had
17 responsibility and my visibility, yes, I would say
18 it is.
19   Q.   And did you play any role in the auditing
20 and logging that is described in this paragraph?
21   A.   The areas under my teams, the areas that
22 they would have had roles, referring back to the
23 change management process, if we brought a new
24 server or application online, that was something
25 that we were to inform the InfoSec team on so that

71

1 they could add it to the log event manager or the
2 SolarWinds event manager, I believe was the later
3 name that we used for it. And so they would add
4 those systems into those event managers to collect
5 those logs. So that would be the -- my primary
6 process that I was aware of.
7   Q.   So are examples of the logs, the audit
8 logs referenced in the auditing and logging
9 paragraph, are they the -- the event manager or the
10 SolarWinds event manager?
11   A.   I believe that would have been the
12 primary system that I was aware of. I know there
13 were other tools that the InfoSec team had under
14 their management, but the primary one that I was
15 familiar with was that, the LEM or SEM product.
16   Q.   Oh, the LEM is referring to the log event
17 manager?
18   A.   That is correct.
19   Q.   I see. Okay. And who in your
20 team -- you mentioned people on your teams were in
21 charge of the LEM or the SEM. Who was that?
22   A.   My team wasn't in charge of LEM or SEM.
23 That fell under InfoSec, but if my team was, let's
24 say, deploying a new server or potentially a new
25 application or firewall or switch, they would alert

72

1   Q.   Okay. And what do you mean by "outputs"?
2   A.   Going into the administrative consoles of
3 our Active Directory server, reviewing accounts,
4 that type of view.
5   Q.   And do you recall providing this document
6 to Mr. Mills?
7   A.   I believe I had sent it to him via e-mail
8 to discuss in one of our one-to-ones or one of our
9 meetings that I had with him.
10   Q.   Do you recall ever presenting this
11 PowerPoint at a meeting?
12   A.   I remember -- I can't remember now
13 because we're going on seven years. I remember a
14 discussion around it and some projects that we
15 kicked off from recommendations and from discussions
16 with the team.
17   Q.   And when you're referring to "team," is
18 it your IT team?
19   A.   I believe -- yes. That would have been
20 my IT systems team that had administration over this
21 area. So that would have been the team that I would
22 be interfacing with.
23   Q.   Okay. Directing you to Bates page ending
24 in 2013.
25   A.   Uh-huh.

93

1   Q.   Do you see at the top it says Current
2 Assessment?
3   A.   Yes.
4   Q.   All right. And you recall preparing this
5 slide, right?
6   A.   Yes, that's correct.
7   Q.   Okay. So you see it says: We have an
8 unnecessary level of risk within our environment.
9   A.   Uh-huh.
10   Q.   What does that mean?
11   A.   In my opinion, and again, I believe I was
12 about a month into this role, as I was looking at
13 our usage of domain administration from my end -- my
14 team, which my team would have been the ones that
15 had domain admin, I felt like we had an ability to
16 reduce their use of domain administration role to
17 reduce exposure to those accounts.
18   Q.   And what do you mean by "exposure to
19 those accounts"?
20   A.   Anytime you're running as an
21 administrative role, there's another level of risk,
22 both from the risk of making an accidental change,
23 because the domain role -- domain admin role has the
24 ability to change a lot of -- well, really all the
25 settings around the way those servers that run our

94

1 Active Directory are running. So the configuration
2 and settings of that. So there's an added risk of a
3 configuration change that may cause a production
4 issue. There's also always the risk that if an
5 administrator account was compromised, that that
6 could be a risk point. So there's just multiple
7 risks with anytime you're running within an
8 administrative role. But it is normal -- normal
9 process of business that you need administrative
10 role to do many of the actions within the job. So
11 that is one of those standard processes, but it's
12 one of those processes that can be a risk.
13   Q.   Okay. So when you wrote: We have an
14 unnecessary level of risk within our environment,
15 the reference to risk meant usage of domain
16 administration?
17   A.   Yes. I was referring to our
18 administrators, which it mentions 15 accounts
19 running as domain admin. So those would have been
20 administrative accounts that our engineers use to
21 work on the Active Directory domain and manage the
22 domain itself.
23   Q.   Okay. And how did you learn that there
24 were 15 accounts running on -- running as domain
25 admin?

95

1   A.   When you view the administration console
2 within Active Directory, you can see all users that
3 are part of a particular group and that gives you an
4 output of every individual that has an admin
5 account.
6   Q.   Okay. And you recall doing that in
7 June -- May or June 2017?
8   A.   Yes, I believe that's where I came up
9 with these particular answers as far as 15 accounts
10 running as domain admin.
11   Q.   And did you review the administration
12 console within Active Directory as part of your
13 process in preparing this slide deck for Mr. Mills?
14   A.   Well, I -- as mentioned, I prepared it
15 for myself and then presented it to him. It was
16 just something that I was putting together. But I
17 believe that's where I got the 15 accounts from,
18 would have been viewing that console.
19   Q.   Okay. And what was your reaction to
20 learning that 15 accounts were running as domain
21 admin in May or June 2017?
22   A.   It's a normal process. I had come from a
23 smaller environment previously where I was one of
24 potentially two admins, right. It was a smaller
25 company. So, you know, that's what I was more used

96

1 to. And at this company we had a larger company.
2 So at this company we had 15 accounts. It wasn't so
3 much the number, it was that there was some recent
4 changes within Active Directory that allowed you to
5 do modeling around a least-privilege basis, which
6 was newer technology, I believe in Server 2012 or
7 Server 2016. And those were -- gave you the ability
8 to implement more granular controls around domain
9 administration.
10   **Q.** Okay. And the second line says: Five
11 domain admin levels service accounts with passwords
12 unchanged as far back as 2007.
13   Do you see that?
14   **A.** I do, yes.
15   **Q.** Okay. Is that consistent with your
16 understanding of domain admin accounts at SolarWinds
17 in May or June 2017?
18   MR. TURNER: Object to form.
19   **A.** Consistent with my -- of those five
20 accounts?
21 BY MS. WARDEN:
22   **Q.** Yeah.
23   **A.** I believe if I put it down, I assume that
24 I would have pulled it off of that console and that
25 would have been accurate, yes.

              97

1   **Q.** Okay. And was this concerning to you?
2   **A.** It depends on how they're handled.
3 So -- and the need for that service account. So
4 service accounts are a very tricky topic
5 and -- within IT is there a necessary account,
6 particularly domain level. And five is a pretty
7 minimal grouping, but the fact that we had those
8 domain-level service accounts, it's something that I
9 wanted to keep an eye on, and so it's something that
10 I wanted to see as far as is there another way that
11 we can tackle those service accounts.
12   **Q.** You said Server 2012 or Server 2016.
13 Were those Microsoft products?
14   **A.** Those would have been -- when speaking
15 about Active Directory, yes, those would be
16 Microsoft products.
17   **Q.** And then the next sentence on Bates
18 ending in 2013 says: System team currently runs as
19 domain admin, high level of risk during routine
20 operations and particularly onboarding and
21 offboarding of personnel.
22   Do you see that?
23   **A.** I do, yes.
24   **Q.** And was that based upon you observing
25 the -- what did you call it, the directory?

              98

1   **A.** Active Directory.
2   **Q.** Yeah. That was based upon your
3 observations of the Active Directory in 2017?
4   **A.** Yes.
5   **Q.** Okay. And tell me, what does this --
6 what does this mean?
7   **A.** So the systems team in the course of
8 their job needs domain admin to do their job, but
9 the risk that's there is that if we had an exit of a
10 personnel in that role, you would obviously have a
11 risk that that person had higher-level privileges
12 than a normal user. So there's more chance for a
13 malicious-type event if you have a disgruntled
14 employee with a domain admin credential versus a
15 standard employee with an admin credential. So
16 anytime you have a higher level of access, it's a
17 higher level of risk.
18   **Q.** But what does high level of risk during
19 routine operations mean?
20   **A.** During routine operations would be what I
21 was speaking to earlier, which means if you have the
22 ability to make a change on anything, you have a
23 higher chance of making a mistake on anything. So
24 just with a higher level of access, you have a
25 higher level of you can change anything in the

              99

1 system. And if you can change anything in that
2 Active Directory system, you could potentially make
3 a mistake that would be impacting to our production.
4   **Q.** Do you recall any next steps being taken
5 to address the issues that you identified in Bates
6 ending in 2013?
7   **A.** Yes. Yeah, we kicked off multiple
8 projects. I can't remember at this point in time if
9 we had already started our dash -- what we called
10 our dash admin project. What that was was creating
11 separate accounts for anybody with a higher level of
12 privilege. And that may have already been in place
13 before I came in, so I can't remember the specifics
14 around those timelines. But we also kicked off
15 what's called a GMSA program. And so GMSAs are
16 managed service accounts that were one of the pieces
17 of technology that Microsoft deployed in their
18 server system of Active Directory. I can't remember
19 the initial server release, if it was 2012 or 2016,
20 but it was sometime around that time frame, that
21 allowed you to move away from passworded service
22 accounts.
23   That technology only works for certain
24 services, so you couldn't deploy it fully. It still
25 can't be deployed fully because it doesn't work for

             100

1 all use cases, but we moved the applicable service
2 accounts that could be moved to a GMSA to a GMSA.
3 So essentially you would never see the password and
4 that password is autorotated by the server system.
5 So it is an improvement of the way that you handle
6 or can handle service accounts.
7   Q.   So this presentation is dated June 2nd,
8 2017. When do you recall the dash admin project
9 being fully implemented?
10   A.   I can't -- as mentioned, I can't remember
11 if they had already started that before I went in
12 there, because I remember we had separate accounts
13 for our network administrators. And so I don't
14 remember what level the dash admin was deployed at.
15 I know that it's still a process that we follow
16 within the business. I just don't remember when it
17 initially started.
18   Q.   Do you recall when the GMSA program was
19 fully implemented?
20   A.   As mentioned, it doesn't apply to all
21 systems. It can't be used in every scenario. So we
22 had done it to, I would say the fullest extent we
23 could, but I can't remember the duration of the
24 project. Because overall there were only five
25 domain admin level accounts, but there were multiple

101

1 just general service accounts that would have had
2 rights to different areas in the business.
3   Q.   Do you recall discussing Bates ending in
4 2013 with Mr. Brown?
5   A.   No, I do not. I don't even -- I don't
6 know if he was with the business at the time or not.
7 I can't remember his start date, but I don't
8 remember discussing this with Mr. Brown. I
9 discussed it with, Dave Mills would have been my
10 normal point of contact.
11   Q.   Take a look at the next page, Bates
12 ending in 2014. Do you see at the top the slide
13 says Path Forward?
14   A.   Uh-huh.
15   Q.   And then under it it says: Implement a
16 least-privileged based administrative model.
17   Do you see that?
18   A.   Yes.
19   Q.   What is your understanding of the term
20 "least-privileged based administrative model" as you
21 used it in this presentation?
22   A.   In this context I was talking about my
23 administrators. There's a -- some newer
24 technologies that allowed for what you call
25 Just-in-Time privilege administration and also least

102

1 privilege, which would mean -- with Just-in-Time,
2 you only receive access to your administrative role
3 when you need it and then it goes away after you're
4 done.
5   With least privilege you would have only
6 rights to the lowest model needed for your role,
7 which depending on your role could be domain admin,
8 but there are other roles that may not require
9 domain admin that could be more granular within the
10 systems administrator team.
11   Q.   When you say "in this context" you're
12 talking about "my administrators," what do you mean?
13   A.   This would have been -- I had just taken
14 on the system administration team. As mentioned, I
15 was new to it. I just had a month with this team,
16 so I was still learning the team and how they
17 worked, but it would have been the system
18 administrators within that group.
19   Q.   Okay. When you were reviewing the
20 information within Active Directory folders, did you
21 have information about who besides your
22 administrators were -- whether they were
23 implementing a least-privilege-based model?
24   MR. TURNER: Objection to the form.
25

103

1 BY MS. WARDEN:
2   Q.   I'll rephrase it. So you mentioned that
3 you looked at documentation or information within
4 Active Directory, correct?
5   A.   Yes.
6   Q.   Okay. In order to form the basis of
7 Exhibit 5?
8   A.   Uh-huh.
9   Q.   Okay. Did you have
10 access -- least-privilege administrative information
11 based on people other than your administrators?
12   MR. TURNER: Object to form.
13   A.   Yes. I would have been aware of other
14 accounts on the system and the model -- the general
15 model, both with onboarding and offboarding as some
16 of my team would have handled some of the onboarding
17 and offboarding tasks dependent upon the request.
18 And then also obviously within my team.
19 BY MS. WARDEN:
20   Q.   Okay. So besides the system
21 administration team, did you learn any information
22 about whether or not least-privilege administrator
23 model was followed --
24   MR. TURNER: Objection --
25

104

BY MS. WARDEN:
 1
 2   **Q.**   -- by others at SolarWinds?
 3   MR. TURNER: Objection to form.
 4   **A.**   Yes. To my awareness, such as the
 5 network team, the way that they worked, that was
 6 something I was intimately familiar with. I would
 7 have had them close to nine months or almost a year
 8 I believe by this point in time. Our model was
 9 fully a least-privilege-based model for the
10 administration of the network team.
11   More granularity was available in the
12 Cisco devices that we were administering. And so
13 that was in place for that team. So that was my
14 awareness there. And then also as a user, just as
15 my normal day-to-day job, before I was given
16 administrative access with the systems team, I only
17 had access to the basic applications that were
18 underneath my role. So I didn't have administrative
19 access until I took on the systems team and then I
20 was given administrative access.
21   MR. TURNER: As I mentioned before, I
22 need to have a call at noon. So if you could just
23 find a breaking point in the next few minutes, I'd
24 appreciate it.
25

BY MS. WARDEN:
 1
 2   **Q.**   So can you tell me why you wrote:
 3 Implement a least-privilege-based administrative
 4 model?
 5   **A.**   Yes. I was very focused -- as mentioned,
 6 I had just taken on the network team. I had had
 7 them for less than a month. I was familiarizing
 8 myself with their environment, the way that they
 9 worked. And I felt like there was an opportunity
10 for us to implement a different type of access for
11 my system administrators.
12   **Q.**   And is it fair to say that SolarWinds did
13 not have a least-privilege-based administrative
14 model as of June 2nd, 2017?
15   MR. TURNER: Objection to form.
16   **A.**   Well, it's context specific. So if I'm
17 talking about my system administrators, they
18 oftentimes needed full domain admin for the job that
19 they did. But I saw an opportunity with some of the
20 newer tech that was being deployed that we had the
21 ability to go into a different privilege model for
22 those users. But this is very specific to that
23 team, the systems administration team that had
24 domain administration for corporate TUL domain.
25

BY MS. WARDEN:
 1
 2   **Q.**   Is it fair to say that system
 3 administrators at SolarWinds did not have a
 4 least-privilege-based administrative model as of
 5 June 2nd, 2017?
 6   MR. TURNER: Object to form.
 7   **A.**   So, again, their role required domain
 8 admin. There were newer tech that was coming out
 9 that could allow the ability for us to apply a more
10 granular privilege model to their role, but we
11 needed to review it. And again, I wrote this a
12 month into that job. So from my point of view, I
13 felt like there was areas that I could identify for
14 improvement and one of those was around that
15 administrative role for a select few system
16 administrators.
17 BY MS. WARDEN:
18   **Q.**   Did you implement a least-privilege
19 administrative model after June 2nd, 2017?
20   MR. TURNER: Object to form.
21   **A.**   We -- I'm trying to remember the exact
22 sequence of events for our system administrators.
23 For our system administrators, many of them still
24 need domain admin and oftentimes work with domain
25 admin. We did implement some technology that

 1 allowed us to do Just-in-Time administration, which
 2 meant that at the point in time that they needed
 3 their administrative role, that role would be
 4 provisioned and then it would be deprovisioned once
 5 they were done doing the task. So it was less of a
 6 least-privilege model for them because they needed
 7 domain admin in their daily work and it was more of
 8 a Just-in-Time deployment, which is a different
 9 piece of technology. So we -- it was a little bit
10 different, there's a little more context to that.
11   MS. WARDEN: We can break,
12 Mr. Turner.
13   MR. TURNER: Appreciate it.
14   THE VIDEOGRAPHER: Going off the
15 record. Time is 11:58.
16   (Recess taken from 11:58 a.m. to
17 1:01 p.m.)
18   THE VIDEOGRAPHER: Back on the
19 record. Time is 1:01.
20 BY MS. WARDEN:
21   **Q.**   Mr. Cline, before the break I had asked
22 you did you implement a least-privilege
23 administrative model after June 2nd, 2017. Remember
24 that?
25   **A.**   Yes, I do.

1   **Q.**   And you said, "We did implement some
2 technology that allowed us to do Just-in-Time
3 administration."
4   **A.**   Yes.
5   **Q.**   Okay. Is Just-in-Time administration a
6 least-privilege-based administrative model?
7   MR. TURNER: Objection to form.
8   **A.**   It is a different type of model. As the
9 name implies, it's a Just-in-Time access model. So
10 it applies access level for administrators, and this
11 is very specific to the context of the IT systems
12 administration team, which their role is systems
13 administration. So we were looking at the
14 Just-in-Time model for their role.
15 BY MS. WARDEN:
16   **Q.**   So my question is, after June 2nd, 2017,
17 are you aware of a least-privilege-based
18 administrative model being implemented at
19 SolarWinds?
20   MR. TURNER: Object to form.
21   **A.**   Again, I have to preface, it's the
22 context of -- it's very context specific, but if
23 we're talking about the system administration team,
24 which was -- there were a few different folks on
25 that team, they would have had a least-privilege

109

1 model around their access levels.
2   In particular we utilize Just-in-Time as
3 one of those ways to achieve a model. It's a
4 different type of model than what you would call a
5 least-privileged.
6 BY MS. WARDEN:
7   **Q.**   So my question is in the sense that you
8 wrote: Implement a least-privilege-based
9 administrative model, in the sense that you meant it
10 in your words in Bates ending in 2014, your -- is
11 your testimony that a least-privilege-based
12 administrative model was implemented for the system
13 administrators after June 2nd, 2017?
14   MR. TURNER: Object to form.
15   **A.**   Yes. And you could argue that it was in
16 place before as well. What I'm referencing here is
17 very specific to the system administrator role and
18 the ability to improve on the model that we had in
19 place for them. In particular, one of those ways
20 was around a Just-in-Time model, but also there's
21 ways to -- with newer technology that is always
22 changing, there's ways to implement that model
23 differently. So it's a very complex topic. Not
24 trying to avoid the question. Sorry. There's just
25 a lot of pieces to that technology.

110

1 BY MS. WARDEN:
2   **Q.**   What process did you follow to implement
3 a least-privilege-based administrative model after
4 June 2nd, 2017?
5   **A.**   There's multiple -- again, multiple ways
6 of implementing a model. Much of that was in place
7 even for the system administrator role that we're
8 talking about specifically in this document that I
9 wrote. Ways that we made improvements were around
10 what we called our dash admin program which is where
11 we provide a secondary set of credentials for
12 anybody that has an administrative role. So that
13 means in their daily work they don't have admin
14 credentials and they only have admin credentials
15 when they need to go and access something that
16 requires administrative privilege. So that's one
17 key way of changing that model.
18   But it's very much a part of the job of a
19 system administrator to have domain admin, but
20 there's ways to make other improvements around that
21 administrative role. And so that's a lot of what
22 we're -- I was referring to in this document.
23   **Q.**   So in Bates ending in 24 -- 2014, you
24 said: No user or service account would use domain.
25   This is under Path Forward: No user or

111

1 service account would use domain admin. Any log-in
2 attempt would trigger an alert, right?
3   **A.**   Uh-huh.
4   **Q.**   Was that your recommendation?
5   **A.**   It was. As mentioned a month into this
6 position as I was reviewing the team.
7   **Q.**   So what do you mean by when you testified
8 it's part of the job of a system administrator to
9 have domain admin?
10   **A.**   Again, it's -- there's a lot of
11 complexity to the Active Directory environment. So
12 certain tasks just require domain admin. It doesn't
13 matter what you're doing -- or it doesn't
14 matter -- if you're trying to make certain changes
15 to an Active Directory domain, it requires domain
16 admin, just period.
17   There's other roles that you can use,
18 some of the newer what were called, well, roles
19 within Active Directory that could do some of the
20 administrative privileges -- or administrative
21 functions without what would be considered a full
22 domain admin. And a lot of that granularity came
23 with the technology over time.
24   And so same thing, it was implementation
25 over time that we were -- that I was referring to as

112

1 let's look at an implementation using those newer
2 roles and groups to build a more granular
3 administrative function.
4   **Q.** Is it fair to say that as of June 2017 if
5 a user logged into a domain admin, that that did not
6 trigger an alert?
7   MR. TURNER: Object to form.
8   **A.** From my awareness, it would have been
9 logged. I don't know that a user would have
10 triggered an alert because that would have been a
11 normal operational role for an admin, for a systems
12 admin. So they would be doing that multiple times a
13 day. So I don't believe we would have triggered
14 normally an alert.
15   If an account was elevated to domain
16 admin that was not previously a domain admin, that
17 did trigger alert at that point in time.
18 BY MS. WARDEN:
19   **Q.** So -- but why did you recommend going
20 forward, the path forward, to be any log-in attempt
21 to a domain admin would trigger an alert?
22   MR. TURNER: Object to form.
23   Go ahead.
24   **A.** This would reference more of the JIT
25 model. That would mean just as a normal daily,

113

1 until they actually needed that role, they would not
2 have domain admin. Whenever they did use domain
3 admin, in that case it would trigger an alert
4 because they wouldn't normally be a domain admin.
5   So referring back to when your account
6 gets elevated, it triggers an alert, this would work
7 in that same manner. So only when they were
8 elevated to domain admin, then it would trigger an
9 alert. So that's the Just-in-Time-type model. It's
10 a different model around providing access.
11 BY MS. WARDEN:
12   **Q.** When was the Just-in-Time model fully
13 implemented?
14   **A.** I can't say fully. And speaking just to
15 the systems team, I know we kicked off a dash admin
16 program, but I don't -- I would have to see one of
17 the forms or project tracking that we did on it.
18 That was a series of programs around building the
19 technology, changing the roles and then implementing
20 that model for the team. So I can't say
21 specifically. I believe we had tackled that project
22 shortly after discussing this, but I'd need to see
23 some documentation on it.
24   **Q.** Okay. The last sentence of the Bates
25 ending in 2014, it says, under Path Forward:

114

1 Implement, manage, service accounts and remove any
2 elevated service accounts.
3   Do you see that?
4   **A.** I do, yeah.
5   **Q.** Why did you say: Remove any elevated
6 service accounts?
7   **A.** This was referring to -- I'd previously
8 referred to managed service accounts, or they later
9 became called GMSAs. They changed over time the
10 technology from Microsoft and the way that you would
11 implement it. But with MSAs -- with MSAs, managed
12 service accounts, or GMSAs, you can deliver those in
13 certain scenarios without elevated privileges.
14   As previously mentioned,
15 there's -- doesn't cover all use cases. And
16 there's generally still needs for elevated service
17 accounts. So once again, I was a month into this
18 position, so I was still reviewing the team, let
19 alone the larger business. So this was just my
20 initial assessment as I had first stepped into that
21 team.
22   **Q.** So the words say: Remove any elevated
23 service accounts.
24   **A.** Uh-huh.
25   **Q.** Are you saying that that -- that was

115

1 incorrect on your part?
2   MR. TURNER: Object to form.
3   **A.** I would say after full assessment,
4 realized that that was not a fully viable path.
5 BY MS. WARDEN:
6   **Q.** Today or you realized that sometime after
7 June 2017?
8   **A.** No. In course of actually working on the
9 projects. Like this is an initial recommendation
10 off of a brief review. So after that I hand it to
11 my engineers and actually dig into the technicals,
12 and then they would come back with their
13 recommendations and viability. So this is just an
14 initial -- my initial concept.
15   **Q.** Were alerts ever put in place when
16 someone tried to log into a domain admin account?
17   MR. TURNER: Object to form, and
18 asked and answered.
19   **A.** From -- yes. From my understanding of
20 it, we alerted off of elevation of an account. I do
21 not -- I cannot recall precisely because I don't
22 handle all of the technical details at that level if
23 there is an alert on every time a domain account's
24 used. That would be under the monitoring of the
25 InfoSec team.

116

1 BY MS. WARDEN:
2   **Q.**   Were you involved in the implementation
3 of alerts going forward after June 2nd, 2017, on
4 domain admin accounts?
5   MR. TURNER: Object to form.
6   **A.**   No, that would generally be, as
7 mentioned, handled by the InfoSec team. And so I
8 might make a recommendation or a request, but
9 generally that would be a decision by the InfoSec
10 team on what they would alert on.
11 BY MS. WARDEN:
12   **Q.**   Did you review individual users'
13 privilege levels as part of this process?
14   MR. TURNER: Object to form.
15   **A.**   Are we speaking specifically to
16 this -- as in this?
17 BY MS. WARDEN:
18   **Q.**   As part of -- in preparing Exhibit 5, did
19 you -- do you recall reviewing individual users'
20 privilege levels?
21   **A.**   No, I do not. And as mentioned, this was
22 in 2017. I don't recall my process for putting this
23 together.
24   **Q.**   Well, you did recall reviewing
25 information in Active Directory?

117

1   **A.**   That was a general statement. I would
2 have had to have reviewed documentation within
3 Active Directory in order to have seen these things.
4 But as far as how I actually did it at the time from
5 seven years ago now, I can't recall my exact steps.
6 But the only way that I would have come to some of
7 these conclusions would have been if I had looked at
8 it.
9   **Q.**   Okay. And then on Bates 2013, just to go
10 back for one second, you referenced 15 accounts
11 running as domain admin.
12   **A.**   Yes.
13   **Q.**   Fifteen accounts out of how many
14 accounts, users' accounts, that you reviewed?
15   MR. TURNER: Object to form.
16   **A.**   So in order to view the domain admin
17 account, you look at the group that's for domain
18 admins and it tells you what user accounts are
19 within that. So you can look at just that account
20 to view it.
21   As far as total accounts within our
22 domain, it would have been into the thousands as far
23 as total user accounts and service accounts across a
24 company of that size. But you would just look
25 specifically at the domain admin group to see how

118

1 many accounts are domain admin.
2 BY MS. WARDEN:
3   **Q.**   Did you make an assessment as to whether
4 the company as a whole had many accounts running as
5 domain admin?
6   MR. TURNER: Object to form.
7   **A.**   As stated here, I had -- apparently had
8 looked at it and it said there were 15 accounts
9 running as domain admin.
10 BY MS. WARDEN:
11   **Q.**   And did you view that as a systemic issue
12 at the company?
13   MR. TURNER: Object to form.
14   **A.**   No, these were my -- these were team
15 administrators. So that was their role. That's
16 their job. Their actual title is system
17 administrator. So that's a -- that is a -- a
18 normal -- would be considered a normal role for
19 their job to have that title.
20 BY MS. WARDEN:
21   **Q.**   But you also said that 15 accounts
22 running as domain admin was an unnecessary level of
23 risk within our environment.
24   MR. TURNER: Object to form.
25

119

1 BY MS. WARDEN:
2   **Q.**   Right?
3   **A.**   It's very contextual. And specifically
4 what I'm stating is that I felt like there was areas
5 for improvement around the administrators and their
6 use of domain admin. So it was a review of the job
7 a month into the position and I was trying to assess
8 what they were doing, how they were doing their job
9 and if there's ways as a leader that I could make
10 improvements. That's my job as a director.
11   **Q.**   And if we go back to slide ending in
12 Bates 2015, it has the timeline. And it says: This
13 needs to be considered a top-priority project. I
14 recommend decreasing or dropping any noncrucial
15 tasks to gain the needed hours.
16   How did you arrive at your conclusion
17 that it was a top-priority project?
18   **A.**   As mentioned, as a -- new to the position
19 and just taking over that team, I saw an area that
20 we could do for improvement and I felt like this was
21 something that we should prioritize.
22   **Q.**   Prioritize in terms of resources
23 dedicated to the issue?
24   MR. TURNER: Objection to form.
25   **A.**   Prioritize as in in our project workload

120

1 can we take and put this higher -- can we put this
2 in our project workload higher up the stack. So,
3 yes, prioritize the project.
4 BY MS. WARDEN:
5   **Q.**   Did you feel like in June 2017 that there
6 were sufficient resources committed to this domain
7 admin issue that you identified?
8   **A.**   So, yeah. So as far as my pitching the
9 project, discussing it with the team and then later
10 on there was a lot of other factors to consider as
11 far as the viability, the technical feasibility and
12 implementation, but, yes, I don't remember having
13 any concerns after presenting the project. So I
14 don't -- nothing stands out to me at this point.
15   **Q.**   So do you recall more resources being
16 dedicated to the domain admin issue after June 2017?
17   MR. TURNER: Object to form.
18   **A.**   So it's my team, right, so I had to -- I
19 had leadership of the team. So it would be my
20 decision to -- how I would allocate my team and
21 resources. So it would have been of course with
22 guidance from my leadership. But it would have been
23 a matter of me making it a priority for my team
24 dependent on where we came out of with the final
25 recommendation.

                        121

1 BY MS. WARDEN:
2   **Q.**   And did Mr. Mills agree?
3   MR. TURNER: Object to form.
4   **A.**   I honestly can't remember the
5 conversation with Mills at this point in time. I
6 don't ever remember receiving any sort of negative
7 feedback from anyone.
8 BY MS. WARDEN:
9   **Q.**   And you referenced when I asked whether
10 you felt like there was sufficient resources
11 committed to the domain admin issue that you
12 identified, you referenced there's a lot of factors
13 to consider as far as viability, technical
14 feasibility, implementation.
15   Does that -- are those factors as -- that
16 relate to whether or not company resources should be
17 dedicated to a particular issue?
18   MR. TURNER: Object to form.
19   **A.**   Well, you always have to assess -- you
20 always have a finite amount of resources, so you
21 always have to assess where it falls within your
22 priority of your projects. I can't recall what
23 projects we were running at this point in time. As
24 mentioned, I had just taken this team, so I was
25 still gaining an understanding of the team. But

                        122

1 from a resource and prioritization perspective, that
2 was generally my decision to make of how I would
3 allocate those resources. And if -- as long as it
4 didn't defer some larger project that maybe was
5 already in works, but that was generally something
6 that was up to my decision.
7 BY MS. WARDEN:
8   **Q.**   Okay. So if you look at No. 1 on the
9 timeline, it says -- you wrote: Perform complete
10 assessment and account audit and then it has a
11 timeline next to it, 24 hours.
12   **A.**   Uh-huh.
13   **Q.**   What was the complete -- first of all,
14 was this done?
15   **A.**   I can't recall in particular to this,
16 again, seven years ago. We do a massive amount of
17 audits, both from our internal audit team and our
18 external audit teams and our internal operational
19 teams. So I would say yes, multiple times. Again,
20 this was a very quick slide that I put together a
21 month into the job.
22   **Q.**   And what would those assessments, what
23 would they have been called?
24   MR. TURNER: Object to form.
25   **A.**   Security assessment. Account audit. I

                        123

1 don't -- we could have named it anything. We've
2 changed the names of things a lot over the course of
3 time.
4 BY MS. WARDEN:
5   **Q.**   Was it someone within your team that you
6 tasked to perform complete assessment and account
7 audit?
8   MR. TURNER: Object to form.
9   **A.**   I would -- most likely, yes, it would
10 have been one of my resources.
11 BY MS. WARDEN:
12   **Q.**   And do you recall receiving any
13 assessments or account audits after June 2nd, 2017?
14   **A.**   Usually at least a few a quarter, if not
15 on a more regular basis. There's all --
16 there's -- there are dozens of audits that the
17 company performed throughout the course of a year.
18 So they're both some by my team and some by external
19 teams. So it's just a course of process for us that
20 the audits was a regular basis.
21   **Q.**   Did you ever circle back to this timeline
22 to evaluate the company's progress toward goal
23 No. 1?
24   MR. TURNER: Object to form.
25   **A.**   I don't know if I came back to this

                        124

1 specific timeline, but normal assessments and audits
2 were a standard part of our processes.
3 BY MS. WARDEN:
4   **Q.**   And what's the significance of the hours
5 next to the numbers?
6   **A.**   Again, if I recall, whenever I put this
7 slide together, shortly into my role, I had taken a
8 quick SWAG at how many hours it may take for an
9 individual to perform this task.
10   **Q.**   Okay. And to your knowledge -- let's go
11 through the other ones. So No. 3: Remove admin
12 rights for all system user accounts.
13   Was this done?
14   **A.**   So this is referring to our system
15 administrators. And removing of admin rights for
16 all roles is -- was not a possible technical thing
17 for us to perform. They wouldn't be able to do
18 their job without using admin rights.
19   **Q.**   Okay. So item No. 3 was not completed?
20   **A.**   Not in that manner, no. As mentioned,
21 very quick assessment that I performed and the
22 ability for them to do everything they need to do
23 within their role required administrative rights.
24 So we couldn't fully remove that.
25   **Q.**   And when did you come to the

125

1 determination that you could not fully remove admin
2 rights for all system users?
3   MR. TURNER: Object to form.
4   **A.**   This isn't all system users. This is
5 specifically speaking about my system administration
6 team.
7 BY MS. WARDEN:
8   **Q.**   I'm sorry, that was my fault. When did
9 you come to the determination that you could not
10 remove the admin rights for your system
11 administration team?
12   **A.**   I can't remember precisely, but I would
13 assume after my technical engineers took a look at
14 the proposal and probably came back to me with a
15 more viable option.
16   **Q.**   And what was that?
17   **A.**   Again, I -- this is seven years ago. I
18 can't remember precisely what this -- because this,
19 as I mentioned, was a very quick assessment that I
20 performed. Very new to the role. I don't remember
21 precisely where we went forward with my system
22 administrators and their accounts and every step
23 that we took between there. Our general focus had
24 become on using a dash admin account hierarchy,
25 which they would only use whenever they needed to

126

1 perform administrative functions. And that was
2 our -- one of the takeaways that I think we came out
3 of this with because that was one of the
4 implementations that we did.
5   **Q.**   After June 2nd, 2017, do you recall
6 anyone above you at the company informing you that
7 you could not remove admin rights for all system
8 user accounts?
9   **A.**   So, again, "all system user accounts" is
10 not the proper phrasing. This is very specific in
11 this slide referring to my system administrators.
12 Their job was to be domain administrators. That's
13 what we paid them and hired them to be part of the
14 company for, was to be a domain administrator. So
15 the idea that we could remove their domain
16 administrative accounts means that they couldn't do
17 their job. So, no, I don't remember anybody coming
18 to me and telling me that my team could not do their
19 job.
20   **Q.**   No. 7 says: Implement alarming of any
21 elevated access.
22   Was this completed?
23   **A.**   From my awareness, this was actually
24 already in place. And I may not have learned it
25 about that until I had been in the role longer, but

127

1 we had an alarm that we've previously discussed that
2 was part of the InfoSec team. They managed the LEM
3 system. They triggered if any rights were elevated
4 to what they considered a privilege level. It
5 wasn't always necessarily domain administrator.
6 There were multiple roles that followed under
7 privilege administration, but domain administrator
8 was one of the functions that they alarmed off of.
9 So, yes, I would say that was completed or already
10 completed prior to my knowledge.
11   **Q.**   Did -- were you aware of any, I guess,
12 additional alarming -- or implementation of
13 additional alerts after June 2nd, 2017?
14   MR. TURNER: Objection to form.
15 BY MS. WARDEN:
16   **Q.**   I understand you said that you -- you
17 believe you were incorrect, right, in your statement
18 that alarms -- there was not alarming of elevated
19 access, right?
20   MR. TURNER: Objection to form.
21   **A.**   So, again, at this point in time, a month
22 into the job, new position, new team, I
23 didn't -- was not fully aware of all the processes
24 that were involved by other teams. But the InfoSec
25 team had multiple alarms and alerts that they

128

1 followed. One of those was elevation of an account.
2   As far as other alerts that they put into
3 replace, yes, it's a continuous evolution.
4 Technology's constantly changing, processes are
5 constantly changing. It's a week-by-week,
6 day-by-day, year-by-year elevation as you're working
7 in technology. And so, yes, there would have been
8 other alerts that would have been put in place in
9 the due course of a year.
10   (Deposition Exhibit 6 marked for
11 identification.)
12 BY MS. WARDEN:
13   Q.   Mr. Cline, you've been presented
14 Deposition Exhibit -- Cline Exhibit 6. For the
15 record, it is Bates SW-SEC00042524-2536. It is a
16 January 11, 2018, e-mail from Kellie Pierce to you
17 and others.
18   Take a moment to review, sir.
19   (Witness reviews document.)
20   A.   Okay.
21 BY MS. WARDEN:
22   Q.   Do you recognize this document?
23   A.   Not specifically. I was -- I am on the
24 e-mail chain, so I'm sure I would have seen it, but
25 I don't necessarily remember this specific version.

                          129

1   Q.   Okay. But you -- you received this
2 e-mail, right?
3   A.   Yes. Appears so, yes.
4   Q.   All right. And if you look at the first
5 page, so it's Bates ending in 2524, the subject says
6 January 11th -- 1/11 user access management notes.
7   Do you see that?
8   A.   Note?
9   Q.   In the subject. In the subject.
10   A.   Oh, in the subject. Yes.
11   Q.   Do you recall attending user access
12 management meetings?
13   A.   User access management meetings.
14   MR. TURNER: Object to form.
15   A.   User access management meetings. I
16 believe so. It lists me as an attendee, so that
17 makes sense, yes.
18 BY MS. WARDEN:
19   Q.   Not focusing on this, just in general, do
20 you recall attending user access management
21 meetings?
22   MR. TURNER: Object to form.
23   A.   A very wide topic. There's a lot of
24 different facets to it. So in the course of
25 business in between our CAB meetings, change of

                          130

1 management meetings, our audits, our external
2 audits, yes, there were multiple user access
3 meetings that I would have been a part of.
4 BY MS. WARDEN:
5   Q.   And then under Attendees you're listed
6 under Brad, right?
7   A.   I believe that's me.
8   Q.   That's referring to you. Okay. Let's
9 just go through who else is on this e-mail. Brody
10 Taylor was in your -- in your team -- on your team,
11 right?
12   A.   In 2018, me and Brody were peers. He had
13 the end user services team that handled onboarding,
14 offboarding. I had the systems team and the network
15 team that were specifically in my management.
16   Q.   Okay. But he wasn't -- didn't have the
17 title director of IT, right?
18   A.   Yes, I believe he was a director -- he
19 was hired as a director of IT. He reported to David
20 Mills and I reported to David Mills. We were both
21 directors of IT.
22   Q.   Rick Holmberg, who is that?
23   A.   Rick Holmberg was, I believe, a director
24 at this time. I can't remember precisely. He
25 reported to Joel Kemmerer under the business

                          131

1 application team. I believe that was his reporting,
2 but can't remember precisely.
3   Q.   Outside of IT team?
4   A.   It was in IT team. Joel Kemmerer
5 reported to Rani.
6   Q.   Okay. Who is Brian Dougherty?
7   A.   Brian Dougherty was, I believe, a
8 architect on the business application team. I'm not
9 sure precisely if he reported to Rick or to Joel.
10   Q.   Okay. And then further down in the
11 e-mail, so Kellie Pierce is writing this e-mail, you
12 see Notes. Then it says, reviewed presentation, and
13 then discuss next steps.
14   Do you see that?
15   A.   Yes.
16   Q.   And then under Next Steps it says: Owner
17 of user access.
18   Do you see that?
19   A.   Uh-huh.
20   Q.   Is this the first time you recall there
21 being, like, next steps relating to the user access
22 issue?
23   MR. TURNER: Objection to form.
24   A.   I believe this is specifically talking
25 about a GDPR-related controls, if I take this topic

                          132

1 I'm on the CC of the e-mail.
2   **Q.**   Okay. Then it says: Once 0365 is
3 deployed, figure out how Azure and SharePoint; no
4 action till 2018, Q3 or Q4.
5   What is that? What are you referring to?
6 I mean, what is that referring to?
7   **A.**   Kellie, I believe, wrote this and took
8 the notes. So I can't remember all the details but
9 we were looking at deploying Office 365. And so we
10 needed to understand if there were any implications
11 under GDPR where we would need additional controls
12 or management in relation to GDPR specifically in
13 that environment.
14   **Q.**   And was there a concern that it could not
15 be implemented until Q3 or Q4 2018?
16   **A.**   I don't see any area for concern. I
17 think she's just saying that I have no action until
18 2018 of Q3/Q4.
19   **Q.**   You wouldn't have any role until then?
20   **A.**   That's the way I would take this
21 phrasing.
22   **Q.**   Okay. And then under concerns it says,
23 resource constraint. What did you understand that
24 to mean?
25   **A.**   GDPR is a very large, I would say

137

1 implementation, and very intensive for a technical
2 team. So anywhere where we, IT corporate, would
3 interface with GDPR regulations would require
4 potentially extra work which would be -- require
5 prioritization or reprioritization of my team and
6 staff.
7   **Q.**   So as of January 2018 was it your
8 understanding that there was not sufficient
9 resources for this GDPR initiative?
10   MR. TURNER: Object to form.
11   **A.**   My understanding is that in our initial
12 assessment of GDPR it was going to be a very large
13 body of work and that was going to put a high
14 workload on the teams that were intersecting with
15 GDPR and GDPR's implementation.
16 BY MS. WARDEN:
17   **Q.**   Are you aware of additional resources
18 being allocated for GDPR?
19   MR. TURNER: Object to form.
20   **A.**   Yes. We kicked off a very large GDPR
21 initiative. It ran for at least 12 months, if not
22 longer. There's a massive amount of documentation
23 around that listing individuals and actions taken
24 for compliance with GDPR. We even had T-shirts for
25 everybody that was on the GDPR team because it was

138

1 such a large body of work for the team to take.
2 BY MS. WARDEN:
3   **Q.**   I'm going to direct your attention to
4 Bates 2526, the next page. Okay. This is the
5 attached slide deck entitled User Access Management
6 dated January 8, 2018.
7   Do you see that?
8   **A.**   I do.
9   **Q.**   Did you prepare this document Bates
10 ending in 2526?
11   **A.**   No, I did not.
12   **Q.**   Do you know who did?
13   **A.**   I do not.
14   **Q.**   Did you contribute to any portion of
15 the -- this User Access Management slide deck?
16   **A.**   I don't recall being part of the creation
17 of the document.
18   **Q.**   All right. If you can look at 2527,
19 Bates ending in 2527, please. Okay. Do you see
20 where it says Problem Statement?
21   **A.**   I do.
22   **Q.**   Okay. If you can read that paragraph to
23 yourself.
24   (Witness reviews document.)
25   **A.**   I can, yes.

139

1 BY MS. WARDEN:
2   **Q.**   Is that first paragraph consistent with
3 your understanding as of January 8th, 2018?
4   MR. TURNER: Objection to form.
5   **A.**   No. From my perspective of the processes
6 that we followed in our UAR access reviews, that is
7 not consistent.
8 BY MS. WARDEN:
9   **Q.**   And why not?
10   **A.**   Because beyond the onboarding and
11 offboarding, which we track through our Web Help
12 Desk and later on the SolarWinds Service Desk
13 systems, we had multiple processes in place around
14 the onboarding and offboarding of users and their
15 accounts.
16   **Q.**   Was there a standardized process in place
17 as of January 2018?
18   **A.**   There was. That's where the Web Help
19 Desk, the SARF that we've referred to, so the
20 systems access request form, and that digital
21 process that flowed through our Web Help Desk
22 managed our onboarding and offboarding of all rights
23 and identity for a standard user.
24   **Q.**   So you don't agree that these were -- you
25 don't agree with the problem statement in this Bates

140

1 ending in 2527?
2   MR. TURNER: Object to form.
3 BY MS. WARDEN:
4   **Q.**   You don't agree that it's a problem as of
5 January 2018?
6   MR. TURNER: Object to form.
7   **A.**   I do not. From my point of view, I did
8 not see these issues.
9 BY MS. WARDEN:
10   **Q.**   Okay. If you can turn to Bates ending in
11 2530, please. Do you see at the top it says
12 Proposed Recommendation?
13   **A.**   Yes.
14   **Q.**   Okay. And under Recommended Solution, it
15 says in yellow: Leverage Azure for user access
16 management and incorporate SharePoint workflows for
17 end users and permission management.
18   Do you see that?
19   **A.**   I do.
20   **Q.**   Okay. So was that not done as of
21 January 2018?
22   MR. TURNER: Object to form.
23   **A.**   So it's referred to on the first page of:
24 Once Office 365 is deployed, figure out how Azure
25 and SharePoint. No action until 2018, Q3 and Q4.

141

1   What that's referencing is our migration
2 into Azure Active Directory. So that was a new
3 migration to a new type of Active Directory that was
4 cloud-hosted.
5   So I believe at the point in time that
6 this slide was created we would not have migrated to
7 Azure Active Directory. I think she's referring to
8 that in the future as an ongoing project.
9 BY MS. WARDEN:
10   **Q.**   And was Azure AD meant to standardize
11 access management controls?
12   **A.**   Azure AD was meant to move us into the
13 cloud, so the goal around that was to provide us
14 with a cloud-based Active Directory rather than an
15 on-prem hosted Active Directory. It wasn't a matter
16 of controls.
17   **Q.**   Well, did Azure AD standardize something?
18   MR. TURNER: Object to form.
19   **A.**   Azure AD gave us a new piece of
20 technology and a new way of managing our user
21 identity. Specifically it was needed for moving
22 into a cloud environment from an on-prem
23 environment.
24 BY MS. WARDEN:
25   **Q.**   Is it fair to say Azure AD was a

142

1 cybersecurity best practice?
2   MR. TURNER: Object to form.
3   **A.**   I don't know if that necessarily has
4 anything do with cybersecurity. Azure AD is just a
5 new type of Active Directory. It's a next
6 generation of technology from Microsoft.
7 BY MS. WARDEN:
8   **Q.**   Is it an Active Directory best practice?
9   MR. TURNER: Object to form.
10   **A.**   It's a new -- it was a new piece of
11 technology. We were implementing a new piece of
12 technology. So the cloud had come out. We were
13 moving to the cloud.
14 BY MS. WARDEN:
15   **Q.**   And when was Azure AD fully implemented?
16   MR. TURNER: Object to form.
17   **A.**   I need to go back to our project slides,
18 but as Kellie referenced, this was around the time
19 that we were moving into Office 365 and Azure --
20 both of those required Azure AD in order for you to
21 provision users into those environments. So if
22 you're moving into Office 365, you have to have
23 Azure AD. We started our move into Office 365
24 sometime in 2018. That would have necessitated
25 Azure AD to make that work.

143

1   (Deposition Exhibit 7 marked for
2 identification.)
3 BY MS. WARDEN:
4   **Q.**   Mr. Cline, you've been presented with
5 what has been marked Cline Exhibit 7. For the
6 record, it's Bates SW-SEC00042892-2964. It is a
7 March 16, 2018, e-mail from you. Take your time to
8 look at it.
9   (Witness reviews document.)
10   MR. TURNER: While the witness is
11 reading the document, I'm going to go grab my
12 glasses.
13 BY MS. WARDEN:
14   **Q.**   I will direct you to certain sections.
15   **A.**   Okay.
16   **Q.**   Okay. So, Mr. Cline, do you recognize
17 this document?
18   **A.**   I recognize the form of the project
19 portfolio. I can't say that I specifically remember
20 this version. It was a normal weekly thing that we
21 would review with our leadership.
22   **Q.**   Okay. And -- all right. You sent this
23 e-mail, right, in document Bates ending in 2892?
24   **A.**   Yes, I sent the e-mail specifically, yes.
25   **Q.**   And you sent it to -- so in March 2018

144

1 before you decided that?
2   A.   I don't specifically recall. I know as
3 mentioned, Eric and some other people are listed on
4 here. I also had passed it on to Bill Carroll. So
5 there's multiple other people that would have been
6 aware of it.
7   Q.   Who is Bill Carroll?
8   A.   He was -- as mentioned previously, he was
9 my leader after David Mills and before I was
10 reporting to Rani Johnson. So he was the senior
11 director of IT during the 2018 time frame.
12   Q.   And then, sorry, the last sentence of his
13 proposal, just to finish this: For everyone else,
14 there could be one or two separate VPN gateways per
15 region with stricter policy (access to less
16 resources).
17   Do you see that?
18   A.   I do.
19   Q.   And did you not agree with that,
20 Mr. Krajcir's proposed there as well?
21   A.   I think ultimately we did agree as
22 reducing our VPN gateways provided a better
23 experience for our end users. And so we did
24 implement some of those recommendations and I saw
25 that as a project that Robert could run and get him

181

1 some visibility to our leadership team.
2   Q.   When was -- when was the proposal
3 relating to one or two separate VPN gateways per
4 region with stricter policy implemented?
5   A.   I would have to go to our
6 management -- our DOIT management portfolio. I
7 don't remember precisely when we did the gateway
8 work.
9   Q.   And was that under your group?
10   A.   Yes, it would have been.
11   Q.   Okay. So your group implemented that
12 change?
13   A.   Yes.
14   Q.   All right. If you can go back to Bates
15 1654. Do you see Krajcir's August 24, 2018, e-mail
16 to you and others?
17   A.   I do.
18   Q.   So this is about two and a half months
19 after Krajcir first e-mails you, right?
20   A.   That seems correct, yes.
21   Q.   Okay. Krajcir writes: I would like to
22 drag your attention back to this topic.
23   So I asked you if you had discussions
24 with Krajcir after his June 4th e-mail. Do you
25 recall talking to him, if this helps jog your

182

1 memory, before he e-mailed you back again on
2 August 24th, 2018?
3   A.   I don't remember specifically. As
4 mentioned, we had both team meetings and we had some
5 one-to-one cadences. And so if we're talking about
6 a month of time lapsed, yes, I would say we would
7 have met --
8   Q.   Two and a half months.
9   A.   Two and a half months, we would have met,
10 yes.
11   Q.   Okay. And you mentioned there was a
12 change that was made from Mr. Krajcir's e-mail, the
13 two separate VPN gateways per region.
14   Was that done prior to August 24th, 2018?
15   A.   As mentioned, I don't remember the
16 precise implementation dates for the gateway
17 modification.
18   Q.   Okay. Krajcir wrote on Bates 1654:
19 Implementing certificates is essential to enforce
20 proper security policies not only on VPN but also on
21 corporate wireless to properly address BYOD problem.
22   Do you see that?
23   A.   I do.
24   Q.   And is BYOD bring your own device?
25   A.   Yes, I believe that's what it would be

183

1 referring to.
2   Q.   Okay. And what do you understand the
3 issue that Krajcir is identifying here? Is it
4 slightly different?
5   A.   No. This is the same topic.
6   Q.   Okay. Which is what?
7   A.   He's referring to attempting to implement
8 certificates on devices joining our VPN to remove
9 the potential for unmanaged devices.
10   Q.   Okay. And what was your opinion as to
11 Mr. Krajcir's sentence there? Did you agree with
12 it, not agree with it?
13   A.   The same as the first e-mail and
14 statement. I did not agree with it.
15   Q.   Okay. Would you describe the
16 implementation of machine certificates to be an
17 industry best practice?
18   A.   No. Machine certificates are easily
19 subverted and at this point in time it was very
20 common in the wild for threat actors to circumvent
21 machine certificates. An end user could also copy a
22 certificate and replicate it. It's not -- it's not
23 a secure piece of technology.
24   Q.   Okay. A little bit further down
25 Mr. Krajcir says: We see -- wrote: We see every

184

1 day that people are accessing our corporate WiFi
2 with their smartphones or other devices that are not
3 joined in the domain. This seems to be common
4 practice.
5   Do you see that?
6   A.   I do.
7   Q.   How common was this practice in your
8 opinion as the network administrator?
9   A.   It was standard to access WiFi.
10   Q.   Standard for people to access SolarWinds'
11 WiFi on their smartphones?
12   A.   Yes.
13   Q.   Okay. And so that was happening in
14 August 2018?
15   A.   Yes.
16   Q.   Was it happening the whole time you were
17 at SolarWinds?
18   A.   Yes. It's how we get on the network.
19   Q.   What are the risks to SolarWinds
20 associated with this practice?
21   A.   The same risk as accessing any piece of
22 software with any device anywhere in the world.
23 It's a standard due course of process. You use your
24 device to access a network and then to access your
25 applications and services.

185

1   Q.   What does not joined in the domain mean?
2   A.   A non-domain joined device just means
3 that device is not joined to the domain. It's just
4 not -- it's not on the domain, not joined to the
5 demain.
6   Q.   Okay. And then Krajcir writes: While we
7 do not have any control over such device (proper
8 antivirus, NetScope, OS updates, et cetera), it can
9 easily reach any resource on any port on our
10 corporate or SW dev network.
11   Do you see that?
12   A.   I do.
13   Q.   What does it mean to reach any resource
14 on any port on our corporate or SW dev network?
15   A.   Again, Robert was very new to the
16 company. He was also a junior engineer. He did not
17 understand what systems were in place. So that's a
18 completely incorrect statement. You cannot access
19 any port or any device on our network from any
20 device. That's just not accurate.
21   Q.   Krajcir wrote then: While on corporate
22 WiFi or VPN such device can basically do whatever
23 without us detecting it until it's too late.
24   Do you see that?
25   A.   I do.

186

1   Q.   Do you agree that this behavior was
2 occurring in August 2018?
3   A.   No, do not.
4   Q.   Why not?
5   A.   So in general -- or not in general, but
6 the way that we had -- the way we had it designed,
7 and this was implementation of our next-generation
8 firewalls that get referred to in multiple places
9 here, I believe. There were zones. We had a couple
10 hundred different zones that would be broken down
11 between offices, within an office, within a device
12 type. And each one of those zones had their own
13 rules regarding what type of traffic could
14 transition from that zone to another zone. And
15 that's where the firewall rules would come into
16 place. So we had multiple both what are called ACLs
17 for each one of those zones depending on if it was
18 considered an adversarial zone or a standard
19 corporate zone, what type of device was on that
20 zone. And at that point in time the firewall, they
21 both looked at the behavior heuristically. If it
22 saw anything normal from a data transmission or
23 session standpoint, it would shut down that session
24 and trigger an alert that went to the InfoSec team.
25   Also by default ports were blocked

187

1 depending on what zone you were traversing and
2 depending on the risk of the type of traffic. So
3 there's a lot of consideration around what can and
4 cannot happen from zone to zone. And that was where
5 a lot of our -- much of our security was that Robert
6 doesn't seem to be aware of when he's writing this.
7   Q.   Did you inform Robert of this?
8   A.   I can't remember if I sat down with him
9 directly and walked him through it. That might have
10 been something that Charles would have done as his
11 manager. As director, my roles were much broader
12 than educating a junior engineer on our environment.
13 That would have been something more for his direct
14 manager.
15   Q.   Can you help me understand these zones?
16 You're saying the zones detect -- the zones detected
17 any devices that were on the network, that were
18 accessing the network?
19   MR. TURNER: Objection to form.
20   A.   Yes. With any firewall or any network,
21 you have what are called VLANs. You break up or
22 segment based on, called IP addresses or CIDR
23 blocks. You break up traffic into generally small
24 contained groups. So the zone may be 128 devices,
25 it may be 256, it may be ten, depending on how you

188

1 decide to approach that zone. So you create zones.
2 And as I mentioned we had literally hundreds of them
3 across our sites and data centers.
4   Depending on the type of device, if it
5 was a wireless device, if it was a phone, if it was
6 a laptop, if it was a server, if it was considered
7 adversarial, meaning an unmanaged device coming into
8 our VPN, they all had different rules that were
9 automatically applied. If it was in an adversarial
10 zone, devices cannot talk to each other on that
11 zone. They may be able to talk out, but only on a
12 specific allowed port. And at that point all
13 traffic packet by packet was scanned by that
14 firewall looking for malicious behavior, potentially
15 a virus, anything that it saw abnormal.
16   We had a subscription with Palo Alto to
17 what was called WildFire, a subscription service
18 that they provided where they were watching globally
19 all of their firewalls across all of their companies
20 and if they saw something suspicious happening in
21 one region, they would send out a heuristical
22 imprint that would get fed to all your devices so
23 that it would also look for that behavior in your
24 region and flag it.
25   That flag, how we handled that in normal

189

1 standard process in our business was that would
2 alert to the InfoSec team and the network team for
3 review so that they could go and look to see what
4 something might be malicious happening within our
5 environment. So that was the zones and how we
6 utilized our next-generation firewalls to manage
7 that and that's why I did not feel like an unmanaged
8 device coming in on VPN was a risk.
9 BY MS. WARDEN:
10   **Q.**   Okay. Further down, just going through
11 Mr. Krajcir's comments, he says -- do you see where
12 it says: It can easily download any content without
13 being detected by NetScope which is normally
14 installed on all domain PCs?
15   Do you see that?
16   **A.**   I do.
17   **Q.**   All right. What is NetScope?
18   **A.**   NetScope is a DLP software I believe is
19 its primary focus, but that was managed by the
20 InfoSec team. So I did not ever have management of
21 it. I'm not intimately familiar with everything
22 that it's capable of doing.
23   **Q.**   Are you aware of whether there's a
24 difference in how quickly NetScope would detect an
25 unmanaged device compared to a managed device?

190

1   MR. TURNER: Object to form.
2   **A.**   NetScope wasn't used for detecting
3 anything having to do with managed or unmanaged.
4 NetScope was a piece of DLP software. So it would
5 look for potentially behavior on that device. So it
6 was just another layer of security, much like
7 antivirus would be on a device.
8 BY MS. WARDEN:
9   **Q.**   Okay. Then further down Mr. Krajcir
10 writes: It can compromise entire networks by
11 spreading malware (spyware, viruses, trojans,
12 ransomware), because we cannot ensure that such
13 device will be fully compliant in terms of OS
14 updates, antivirus, software installed, et cetera.
15   Did you agree with Mr. Krajcir's opinion?
16   **A.**   I did not. Referring to my earlier
17 description of how the firewall worked from zone to
18 zone, we would see any sort of virus-type activity
19 traversing a zone or in a normal session egressing
20 our WiFi or any of our zones. So that risk we did
21 not feel -- or I did definitely not feel was there
22 with those other controls in place.
23   **Q.**   Because the firewalls were sufficient in
24 your opinion?
25   **A.**   Yes.

191

1   **Q.**   Okay. Further down Mr. Krajcir says: We
2 know that sometimes people are leaving the company
3 but their AD credentials remain active for a few
4 more days.
5   What did you understand the issue that
6 Mr. Krajcir was identifying?
7   **A.**   Well, he's trying to say that somebody
8 may leave and their account may still be active.
9 But once again, junior engineer, six months on the
10 job. He did not work on the team that handled
11 onboarding and offboarding, so I don't know where he
12 would have come to this conclusion.
13   **Q.**   So you don't agree that this behavior was
14 happening in August 2018?
15   **A.**   No, I do not. We had multiple controls
16 and audits in place around our onboarding and
17 offboarding.
18   **Q.**   All right. At the end he has another
19 proposal. This is the August 24, 2018, proposal.
20 He suggests: Trim down user admin rights so that
21 they won't be able to export certificates on their
22 PC.
23   Do you see that?
24   **A.**   I do.
25   **Q.**   What has been done to reduce admin rights

192

1 as of August 2018? What had been done to reduce
2 admin rights?
3   MR. TURNER: Object to form.
4   A.   So to be clear, he's talking about
5 administrative rights on your local device. So
6 that's the ability to add a printer, join the WiFi,
7 change your wallpaper. Those are normal rights that
8 a user needs on their desktop to do their job. So
9 removing admin rights was not an option and not a
10 good recommendation. And especially to do that to
11 manage certificates, which was an outdated piece of
12 technology, was not a good recommendation.
13   So, yes, users had local admin rights
14 strictly to their device so that they could change
15 their wallpaper, add a printer. And that was the
16 extent of those administrative rights for a standard
17 user.
18 BY MS. WARDEN:
19   Q.   Why did you interpret Mr. Krajcir's
20 reference to admin rights to be local admin rights?
21   A.   Because the only users in our environment
22 that had admin right -- the only place where a user
23 would have had admin rights is to their laptop or
24 device. As discussed previously, as I called out in
25 my slide around systems administrators, generally

193

1 only systems administrators or, like, the 15 users
2 that I had responded to -- or described in that
3 slide were the only people with actual domain admin
4 rights, which is strictly speaking an Active
5 Directory thing. So there's a lot of different
6 administrative rights and he's talking about their
7 PC. So he's talking about local PC administrative
8 rights.
9   Q.   Mr. Krajcir also proposes enroll
10 certificates.
11   Do you see that?
12   A.   I do.
13   Q.   Okay. What's your opinion with respect
14 to that?
15   A.   The same as previously. This would be
16 the machine certificates that was not a secure piece
17 of technology, was not an improvement.
18   Q.   Okay. So no work had been done as of
19 August 2018 to enroll certificates, correct?
20   MR. TURNER: Object to form.
21   A.   If we get into certificates, we're
22 talking about a lot of different places that you
23 enroll certificates. So if we're talking about the
24 context of PCs, there were domain certificates that
25 we utilized for different functions within the

194

1 business. What he's specifically, I believe,
2 referring to is a machine certificate in relation to
3 VPN access. As mentioned, we did not see that as a
4 secure piece of technology and we did not see it as
5 an improvement to our environment.
6 BY MS. WARDEN:
7   Q.   Third thing Mr. Krajcir suggests is set
8 VPN and wireless policies to accept only devices
9 with valid certificate and with valid AD
10 credentials.
11   Do you see that?
12   A.   I do.
13   Q.   What was your reaction to this proposal?
14   A.   Same as all of his others around
15 certificates. It's not a viable option and it did
16 not improve, in my opinion, security in any way.
17   Q.   Going back to the -- briefly to the
18 enroll certificates suggestion that Mr. Krajcir had.
19 What was your understanding as to whether users
20 could export certificates on their PC as of
21 August 24th, 2018?
22   A.   If you have local administrative rights,
23 or even without them, there are ways to export a
24 certificate from a machine. You can then copy that
25 file over to another device and potentially

195

1 duplicate that certificate. So it's just a file
2 that can be copied and duplicated.
3   Q.   What kinds of certificates?
4   MR. TURNER: Objection to form.
5   A.   In this context?
6 BY MS. WARDEN:
7   Q.   Yeah. What kinds of certificates could
8 be exported to a PC?
9   A.   Any. Any certificate. That's why it's
10 not a secure piece of technology.
11   Q.   Did you see that as a security risk?
12   MR. TURNER: Objection to form and
13 asked and answered. He's been over this, again, ten
14 times at least.
15   A.   Did I see -- I saw relying on
16 certificates as a security risk in this -- in the
17 context that he is describing here.
18 BY MS. WARDEN:
19   Q.   Was the fact that users could expert
20 certificates on their PC as of August 24, 2018, did
21 you see -- did you view that as a security risk?
22   MR. TURNER: Objection to form, asked
23 and answered. You're not listening to the witness.
24   A.   No, I did not believe certificates were a
25 function. Whether you are -- that would pose a

196

1 security risk if you could copy that
2 certificate -- it's not a secure piece of
3 technology. You don't want to rely on certificates.
4   MS. WARDEN: The court reporter would
5 like to break, so let's break.
6   THE VIDEOGRAPHER: Going off the
7 record. Time is 3:33 p.m.
8   (Recess taken from 3:33 p.m. to
9 3:53 p.m.)
10   THE VIDEOGRAPHER: Back on the
11 record. Time is 3:53.
12 BY MS. WARDEN:
13   Q.   Mr. Cline, can you turn to the very first
14 page of Exhibit 9, Bates ending in 1653, please.
15   A.   Yes.
16   Q.   Okay. Does this appear to be an August
17 30th, 2018 e-mail from Robert Krajcir to you and
18 others?
19   A.   Yes.
20   Q.   Okay. It's a continuation of an e-mail
21 chain we've been discussing?
22   A.   Yes, correct.
23   Q.   Okay. So Mr. Krajcir writes: Please
24 find attached the presentation I used today so you
25 can show to anyone you deem appropriate.

197

1   Do you see that?
2   A.   Yes.
3   Q.   Do you see that language?
4   Okay. Was there a -- did Mr. Krajcir
5 share the PowerPoint starting in Bates 1659 on some
6 kind of WebEx or video platform with you on
7 August 30th, 2018?
8   A.   He lists the attendees here and I'm not
9 on the list of attendees.
10   Q.   Okay. Have you -- but are you aware of
11 it happening?
12   A.   I mean, I am in --
13   Q.   Were you told about it?
14   A.   I can't recall specifically in 2018.
15   Q.   Okay. So if you can just turn to the
16 slide deck, so it starts at 1659 and it goes to
17 1668.
18   A.   Yes.
19   Q.   Can you just briefly flip through it -- I
20 mean, I realize you have already testified that you
21 didn't agree with Mr. Krajcir's comments, so I don't
22 want to waste your time, but briefly flip through it
23 and I'll ask you if there's anything else that
24 Mr. Krajcir brought up in this presentation that he
25 did not already bring up in your e-mails that was

198

1 concerning to you.
2   A.   And specifically the e-mails attached?
3   Q.   Yeah.
4   (Witness reviews document.)
5   A.   No, I do not see any particular
6 statements that are concerning to me.
7 BY MS. WARDEN:
8   Q.   Did you participate in any calls or
9 meetings to address the risks detailed in
10 Mr. Krajcir's BYOD solution PowerPoint?
11   A.   Not beyond the e-mail communications. I
12 don't remember a specific -- as mentioned, we did
13 spawn some projects based around the gateways. And
14 then he's referencing some Office 365 items, so
15 there would have been other intersecting projects
16 potentially that would have overlapped with some of
17 the statements here. But I don't remember a
18 specific meeting beyond the conversations that
19 were -- would have been in just our normal team
20 meetings and in the e-mail communications.
21   Q.   After August 30th, 2018, did Mr. Krajcir
22 bring up the issues identified in the BYOD
23 PowerPoint to you?
24   MR. TURNER: Object to form.
25   A.   I believe he did because we had -- as

199

1 mentioned, I had seen this as a coaching opportunity
2 for Robert. I met with him on site in Brno later in
3 that year and I believe, if I recall correctly, we
4 had a pretty long conversation because we were late
5 to meeting the team for dinner, just generally
6 around leadership, leadership potential, some of the
7 programs and projects he was running. So it may
8 have been covered in our discussions face-to-face at
9 that time, but, again, 2018 I can't recall precisely
10 all my conversations with him.
11 BY MS. WARDEN:
12   Q.   Did Mr. Krajcir ever tell you whether he
13 felt like SolarWinds properly addressed the concerns
14 that he raised in the BYOD PowerPoint?
15   A.   I don't -- I don't recall that specific
16 type conversation.
17   (Deposition Exhibit 10 marked for
18 identification.)
19 BY MS. WARDEN:
20   Q.   You have been presented Cline Exhibit 10.
21 For the record, it's SW-SEC00031564 through 69. At
22 the top it says 2H 2019 CTL/DOIT R4R Goals.
23   Take a minute to review it, sir.
24   (Witness reviews document.)
25   A.   Okay.

200

1 recall, when I directly joined in 2016, there was
2 security training. It was a regular occurrence.
3   (Deposition Exhibit 11 marked for
4 identification.)
5 BY MS. WARDEN:
6   **Q.**   Mr. Cline, you've been presented Cline
7 Exhibit 11. For the record, it's SW-SEC00031499
8 through 57. It is a October 29, 2019, e-mail from
9 you to Rani Johnson attaching a slide deck. Take
10 your time looking at it.
11   (Witness reviews document.)
12   **A.**   Okay.
13   **Q.**   Okay. Do you recognize this document,
14 sir?
15   **A.**   Yes, I recognize the general document.
16 BY MS. WARDEN:
17   **Q.**   Okay. Does this appear to be an e-mail
18 from you to Rani Johnson on October 29, 2019?
19   **A.**   Yes.
20   **Q.**   All right. If you turn to Bates ending
21 in 1500, there's an attached slide deck to this
22 e-mail entitled Monthly Ops Review September 2019.
23   Do you see that?
24   **A.**   I do.
25   **Q.**   This was sent -- this e-mail was sent one

217

1 month before you left the role of director of IT,
2 correct?
3   **A.**   That sounds correct, yes.
4   **Q.**   Okay. Did you prepare the slide deck
5 entitled Monthly Ops Review?
6   **A.**   No. I would have had a portion on it
7 that I would have made adjustments to and I would
8 have supplied that.
9   **Q.**   Okay. Who had primary responsibility
10 over the monthly ops review?
11   **A.**   It would have consisted among a few dozen
12 people underneath Rani Johnson amongst their
13 different areas. So I can't speak to everyone who
14 would have had a piece in this, but it would have
15 all been primarily those teams reporting to Rani.
16   **Q.**   Okay. Do you recall discussing monthly
17 ops reviews on a particular cadence?
18   MR. TURNER: Objection to form.
19   **A.**   We had those monthly.
20 BY MS. WARDEN:
21   **Q.**   Okay. And who attended those?
22   **A.**   As mentioned, primarily Rani Johnson's
23 staff. So if I recall the ones that attended, it
24 was generally a pretty large meeting, both local and
25 remote folks.

218

1   **Q.**   Was Tim Brown present?
2   MR. TURNER: Objection to form.
3   **A.**   As mentioned, they were monthly. I can't
4 speak to every meeting or what the attendance was,
5 so I would say --
6 BY MS. WARDEN:
7   **Q.**   Did Mr. Brown typically attend these
8 monthly ops reviews?
9   **A.**   I don't remember when these started. As
10 mentioned, it was the month before I left. I can't
11 remember if we had started it earlier than that. So
12 I cannot recall the attendees in person at these
13 meetings.
14   **Q.**   Okay. If you can turn to Bates 1527. Do
15 you see at the top it says Lessons Learned/Problems
16 September 2019?
17   **A.**   Yes.
18   **Q.**   Okay. You mentioned you worked on some
19 of the slides. Is this Bates ending in 1527 a slide
20 that you recall working on?
21   (Witness reviews document.)
22   **A.**   I cannot recall if I specifically worked
23 on this slide.
24 BY MS. WARDEN:
25   **Q.**   Okay. Do you see where it says

219

1 Incomplete/Inconsistent Monitoring?
2   **A.**   Yes.
3   **Q.**   All right. And under it says:
4 Incomplete monitoring for critical services or
5 features of a service have -- says lead to
6 approximate poor reaction time for outages or
7 service degradations.
8   Do you see that?
9   **A.**   I do, yes.
10   **Q.**   Is that an accurate reflection of
11 SolarWinds monitoring as of September 2019?
12   MR. TURNER: Objection to form and
13 foundation.
14   **A.**   A, I don't have full context. The
15 context of this slide in particular is talking about
16 our TDF blended circuit and issues that we were
17 experiencing within that particular data center and
18 with that particular circuit. So I don't remember
19 the exact details or even if I put this slide
20 together, but I would not say that's representative
21 of some wider situation. It's talking about TDF.
22   We were -- we created network monitoring
23 software. That's what we did as a business.
24 There's 30 slides in here on us talking a SWOC and
25 the level of monitoring that we do within our

220

1 network. So our maturity of our monitoring was
2 extreme. The standards that we had was extreme
3 compared to the normal because we wanted to lead the
4 way in how we monitor and how we used our products.
5 BY MS. WARDEN:
6   Q.   Is it fair to say you don't agree with
7 that statement?
8   MR. TURNER: I'm sorry. Objection to
9 form.
10   A.   Yes, I believe if I didn't make it clear,
11 I object to that as a blanket statement. It has a
12 specific context.
13 BY MS. WARDEN:
14   Q.   Okay. Do you have any familiarity with
15 the incidents on the right column, Related
16 Incidents? Were they in -- were they in your area
17 of responsibility?
18   A.   Potentially if this is talking about
19 traffic ingressing or egressing from our TDF and to
20 other regions, then there is a chance that as we
21 were having circuit issues on a blended circuit in
22 our data center, TDF is our Texas Data Foundry data
23 center. And if there was something there with a
24 firewall or other issue that caused an interruption,
25 that's what we're referencing that we had an

221

1 interruption in service.
2   One note here as I think about this
3 further. TDF did not allow us to monitor their
4 circuits. So we could only monitor our network and
5 our gear. So our ability to monitor their gear was
6 not allowed. So we had a spot that we could not
7 monitor to the same level that we monitor our
8 internal-owned SolarWinds equipment. And so that's
9 very possibly what this may have been referring to.
10 Because I remember us having issues with our blended
11 circuit there in Data Foundry and it was a
12 consistent issue that had us move away from using
13 that service as our primary network for Texas Data
14 Foundry.
15   Q.   So for the slide in Bates 1527, I
16 understand that you don't agree with the statement,
17 Incomplete monitoring for critical services, but are
18 you aware of any steps taken around the time of this
19 slide deck that you sent to the CIO, okay, in
20 October 2019, are you aware of any steps to address
21 this slide that identified incomplete monitoring for
22 critical services?
23   MR. TURNER: Objection, asked and
24 answered. You're continuing not to listen to what
25 the witness is telling you.

222

1   MS. WARDEN: Same objection to
2 Mr. Turner.
3   A.   Specifically the context of this slide
4 refers to Texas Data Foundry blended circuit. We
5 were not allowed to monitor Texas Data Foundry's
6 blended circuit. It was their equipment. They
7 would not allow us to monitor. If they allowed
8 every one of their customers to monitor it, we would
9 cause a DDoS attack and take their equipment down.
10   So, yes, we could not monitor their
11 equipment. So I do not see anywhere else that this
12 applies but in this context, which is Texas Data
13 Foundry as listed at the very top of the slide.
14   (Deposition Exhibit 12 marked for
15 identification.)
16 BY MS. WARDEN:
17   Q.   Mr. Cline, you've been presented with
18 Cline Exhibit 12. It's for the record Bates
19 SW-SEC00008996 through 97. It is an October 30th,
20 2020, e-mail from Chris Day to you and others. Take
21 as much time as you need to review.
22   (Witness reviews document.)
23   A.   Okay.
24 BY MS. WARDEN:
25   Q.   You received this -- sorry. Do you

223

1 recognize this document?
2   A.   Yes. I believe I've seen it before.
3   Q.   And you received this e-mail from
4 Mr. Day?
5   A.   That appears to be correct, yes.
6   Q.   October 30th, 2020, is the month you
7 rejoined SolarWinds as senior director of IT, right?
8   A.   That's correct.
9   Q.   Okay. So Mr. Day wrote to you: All, see
10 attached. Q4 risk report.
11   And then if you see towards the bottom it
12 mentions Brad, dash, slide 6 low score on BCP.
13   Do you see that?
14   A.   Yes.
15   Q.   All right. Do you recall contributing to
16 the quarterly risk review slide deck that is
17 attached to this e-mail dated October 27, 2020?
18   A.   I do not see any slides that look
19 familiar to me as far as that I would have worked
20 on.
21   Q.   Let's take a look at slide 6 since that's
22 what Mr. Day referenced in the e-mail. So it
23 doesn't have a Bates, but it has 6 at the bottom.
24 Do you see that?
25   A.   Yes.

224

```
 1              REPORTER'S CERTIFICATION
 2        I, Micheal A. Johnson, Registered Diplomate
 3   Reporter and Notary Public in and for the State of
 4   Texas, certify that on the 1st day of October, 2024
 5   I reported the Videotaped Deposition of BRAD CLINE,
 6   after the witness had first been duly cautioned and
 7   sworn to testify under oath; said deposition was
 8   subsequently transcribed by me and under my
 9   supervision and contains a full, true and complete
10   transcription of the proceedings had at said time
11   and place; and that reading and signing was not
12   requested.
13        I further certify that I am neither counsel
14   for nor related to any party in this cause and am
15   not financially interested in its outcome.
16        GIVEN UNDER MY HAND AND SEAL of office on
17   this 7th day of October, 2024.
18
19        _____
          MICHEAL A. JOHNSON, RDR, CRR
20        NCRA Registered Diplomate Reporter
          NCRA Certified Realtime Reporter
21
          Notary Public in and for the
22        State of Texas
          My Commission Expires:  8/8/2028
23
24
25

                    233
```

IN THE UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

SECURITIES AND EXCHANGE COMMISSION,)
)
               Plaintiff,   )
)
               v.   )   Civil Action No. 1:23-cv-09518-PAE
)
SOLARWINDS CORP. and TIMOTHY G.   )
BROWN,   )
)
               Defendants.   )
)
)

<u>Notice of Errata – Deposition of Brad Cline</u>
<u>(October 1, 2024)</u>

       I, the undersigned, do hereby declare that I have read the deposition transcript of Brad Cline dated October 1, 2024 and that to the best of my knowledge, said testimony is true and accurate, with the exception of the following changes listed below:

Page	Line(s)	Change		Reason
		From	**To**	
43	4	a logging event manager	Log Event Manager	Clarification
53	16	statements over the year	statements over the years	Transcription Error
74	11	was that that	was that	Clarification
115	15	there's — doesn't cover	this doesn't cover	Clarification
129	3	replace	place	Transcription Error
129	6	elevation	evolution	Transcription Error

Page	Line(s)	Change		Reason
		From	**To**	
187	20	the firewall, they	the firewalls, they	Transcription Error
187	22	saw anything normal	saw anything abnormal	Transcription Error

I declare under penalty of perjury that the foregoing is true and correct.

Date: ___11 - 12 - 24___   Signed: _____

2